УДК 343.9.01
DOI 10.52452/19931778_2022_4_106

КИБЕРПРЕСТУПНОСТЬ: ПОНЯТИЕ, ПРИЗНАКИ, ОСНОВНЫЕ НАПРАВЛЕНИЯ ПРОТИВОДЕЙСТВИЯ

© 2022 г. ***В.Б. Клишков, Е.В. Стебенева, М.А. Яковлева***

Санкт-Петербургский университет Министерства внутренних дел России, Санкт-Петербург

klishkov63@mail.ru

Поступила в редакцию 29.05.2022

Цель статьи – исследование дефиниции, характерных признаков и основных направлений противодействия киберпреступности. Осуществлен анализ категории «киберпреступность», уровня общественной опасности киберпреступлений; обобщены позиции в отношении характерных признаков данного деяния; представлена классификация киберпреступлений. *Результаты*: в статье нашли отражение особенности наиболее общественно опасных киберпреступлений, представлены их статистические данные (в динамике), авторское видение в отношении дефиниции и признаков данного явления, основные направления противодействия киберпреступности в Российской Федерации.

Ключевые слова: безопасность, киберпреступность, киберпреступление, киберугрозы, личность киберпреступника, противодействие преступности.

В современном обществе развития инновационных технологий, активного использования возможностей сети Интернет, как децентрализованной мировой системы многоаспектных информационно-телекоммуникационных сетей, характеризующихся специальным назначением по целевой трансляции информации посредством вычислительной техники и современной связи [1, с. 7], происходит криминализация информационной среды и трансформация социального явления преступность – в киберпреступность.

Киберпреступность, признаваемая довольно серьезной проблемой всего современного мирового сообщества, наносящей существенный ущерб как национальной, так и мировой экономике, безопасности, может быть выражена в «классических» деяниях, совершенных в киберпространстве посредством применения информационно-телекоммуникационных технологий, характеризуясь как высоким уровнем латентности, так и масштабности, обусловленной совершением преступления в любом месте расположения сетевых структур, применения названных технологий и подключения к сети Интернет [2, с.81]. Киберпреступности свойственны сложности расследования (поиск субъекта преступления, возмещение причиненного материального ущерба и пр.).

В докладе Совета Европы в отношении проблем в области кибербезопасности, киберпреступности и ее классификации киберпреступление определено в качестве общественно опасного деяния, совершенного в информационно-телекоммуникационной сфере посредством применения информационно-коммуникационных технологий [3], т.е. при помощи компьютерной системы либо сети, непосредственно – в названной системе либо сети, либо против названных объектов [4]. Данный вид деяний отражен как CIA-offences, т.е. как общественно опасные посягательства, направленные как против приватности (конфиденциальности; confidentiality), так и единства (целостности; integrity), а также против открытости (availability) данных и информационных систем.

К группе киберпреступлений причислены: во-первых, компьютерное хакерство, во-вторых, шпионаж, реализуемый путем применения «троянских коней» и иных подобных информационных технологий, в-третьих, перехват информационных сообщений, в-четвертых, обман пользователей сети Интернет (включая сферу спуфинга, фишинга), в-пятых, диверсии в компьютерной сфере, как и вымогательство (в т.ч. посредством применения компьютерных вирусов, червей, различных DoS-атак, технологий спамминга и мейлбомбинга) [5, с.225].

В научном сообществе киберпреступления, в широком смысле, обозначены как общественно опасные деяния, посягающие, помимо компьютерных систем, на иные объекты, к основным из которых относятся: национальная и мировая безопасность (кибертерроризм), имущество, имущественные права индивидов и их коллективных образований (это и кражи, и мошенничество, совершенные посредством компьютерных систем или в киберпространстве, а также посягательства на авторские права (плагиат и киберпиратство), на личную безопасность (явления кибербуллинга и секстинга, груминга и троллинга) и пр. [6].

Характерными признаками киберпреступлений являются не только общественная опасность, но и оперативность совершения деяния, удаленность, а также масштабность и высокая анонимность, отражающаяся не только в сложности обнаружения виновного, но и в вероятности предоставить информацию потребителю, не соответствующую действительности. Такой признак киберпреступности, как самодостаточность, облегчает совершение и сокрытие посягательства, а признак виртуальности характеризует место деяния в качестве идеальной не опознанной с точностью среды для «трансформации» личности преступника, перевоплощения и корректирования характеристик (внешнего вида и пр.).

В связи с тем, что определенная часть киберпреступлений остается вне поля зрения правоохранительных органов, данным посягательствам свойственен признак латентности, характеризующийся как объективное социально-юридическое явление, которому свойственны отдельные и качественные, и количественные особенности. Латентная киберпреступность, соответственно, – комплекс деяний, совершенных с применением информационно-телекоммуникационных технологий, которые признаны не выявленными и (либо) не учтенными национальными правоохранительными органами на определенной территории в соответствующий период времени [7, с. 54].

Социально-правовая обусловленность внимания к обозначенным проблемам связана с высоким ростом преступлений, совершаемых с использованием информационно-коммуникационных технологий или в сфере компьютерной информации. Так, за 2020 г. в Российской Федерации рост подобных деяний составил более 70%, в частности, март: +33.7%, апрель: +31.5%, май: +25.7%, июнь: +20.3% [8]. В 2021 г. практически каждое четвертое преступление в России было совершено с использованием IT, при этом темп роста их количества в определенной степени замедлился. Так, если в первом полугодии 2021 г. количество данных деяний увеличилось на 20.3%, то за 9 месяцев 2021 г. года увеличение таких преступлений составило 8.1%. В 33000 преступлений жертвами признаны несовершеннолетние, примерно в 40000 – пенсионеры, в 1400 – лица – инвалиды I и II группы [9].

В указанной связи многогранные проблемы в сфере обеспечения безопасности в киберпространстве отражаются в фундаментальных технических и юридических, стратегических разработках, способствующих нивелированию угроз деструктивного воздействия сети Интернет на личность и в целом на криминальную среду в киберпространстве [10, с. 14]. Вопросы информационной безопасности рассматриваются на высоком государственном уровне. Так, Президент РФ В.В. Путин на расширенном заседании коллегии МВД России (3 марта 2021 г.) отметил наличие многоаспектных угроз в интернет-пространстве и указал на необходимость усиления профилактических мероприятий со стороны правоохранительных органов по противодействию киберпреступности, в целом на более совершенное межведомственное сотрудничество, включая сферу мониторинга пространства сети Интернет, оперативного реагирования на новые криминальные киберугрозы, нацеленные как на мировую, национальную, так и на личную безопасность [11].

С целью реализации направлений противодействия криминализации интернет-пространства в Российской Федерации принята система нормативных источников права, в т. ч. в рамках важнейших для государства, общества, отдельной личности стратегических документов [12–16].

Актуальность киберугроз, обусловленная ростом киберпреступности как нового общественно опасного деяния, активизирующегося на мировом и национальном уровне [17], повлияла на эволюцию международного сотрудничества в обозначенном направлении. Российская Федерация является участницей Конвенции о преступности в сфере компьютерной информации [18], выступает инициатором принятия на уровне Организации Объединенных Наций новой Конвенции о противодействии использованию информационно-коммуникационных технологий в преступных целях [19], проект которой в рамках Резолюции ООН [20] был направлен в Совет Безопасности ООН (июнь 2021 г.).

Направления противодействия негативным процессам, связанным с киберугрозами, отражены в основных целях названной Конвенции: содействие формированию и совершенствованию мер, имеющих направленность на противодействие противоправным деяниям в информационно-телекоммуникационном пространстве; на профилактику киберпреступности; на предотвращение противоправных актов, имеющих направленность против как конфиденциальности, так и целостности и доступности информационных технологий и на предупреждение многоаспектных угроз при их использовании. Данные меры должны быть обеспечены системой национальных мер, в частности, посредством криминализации деяний, которым противостоят положения Конвенции; формирования новых полномочий, призванных к качественному противодействию киберпреступности путем внедрения современных систем обнаружения, расследования, результативного пре-

следования киберпреступников на национальном и межнациональном уровнях, в т.ч. используя межведомственное и межнациональное взаимодействие (подготовка профессиональных кадров, предоставление технической поддержки и пр.).

Проект Конвенции учитывает систему современных киберугроз в сфере информационной национальной и мировой безопасности, расширяет спектр киберпреступлений, необходимых для криминализации в национальном праве. Обращается особое внимание на сферу криминального применения криптовалюты, которая помимо различных электронных средств платежа используется как предмет преступного посягательства при совершении мошенничества [21, с. 121], как и на сферу склонения индивида к самоубийству либо доведения до совершения самоубийства, изготовления и незаконного оборота материалов порнографической направленности в отношении детей.

В Конвенции уделено внимание вопросам вовлечения лиц возраста несовершеннолетия в преступную деятельность и в совершение актов, опасных для жизни, здоровья, некоторым другим, в частности, обусловленным негативным влиянием на личность идей нацизма, геноцида, экстремизма и терроризма, как и угроз, обусловленных распространением в сети Интернет наркотических средств и психотропных веществ, незаконным оборотом оружия и боеприпасов, взрывных средств, нарушением интеллектуальных прав и пр.

Современные национальные реалии обусловливают новые формы преступных проявлений при совершении посягательств посредством применения технологий цифрового общества, в т. ч. сети Интернет, во время пандемии коронавирусной инфекции COVID-19. Активное распространение в указанной связи получили разнообразные виды мошенничества, опосредованные фактами фиктивной вакцинации, подделкой медицинских противопоказаний от вакцинации, соответствующих сертификатов, QR-кодов, подтверждающих факт вакцинации; фактами внесения неправдивой информации в государственную систему отчетности (ст. ст. 159, 236, 327 УК РФ и пр.). По названным составам в г. Москве возбуждено более 50 уголовных дел [22].

Значительная часть киберпреступлений представляет собой кибератаки, которые выражаются в незаконном вмешательстве в различные информационные системы юридических, физических лиц, проявляющемся во взломе как интернет-сайтов, так и приложений, индивидуальных аккаунтов и технических устройств. Разновидности кибератак многоаспектны: это и внедрение различных вирусных продуктов, и рассылка интернет-сообщений и писем, содержащих вредоносные элементы (коды), способствующие незаконному завладению индивидуальными сведениями (фишинг), и кибератаки в аспекте уязвимости, не выявленные своевременно разработчиками, установщиками программ.

Так, общепризнан факт причинения в 2017 г. вирусом WannaCry значительного ущерба многочисленным личным и корпоративным компьютерным системам во многих государствах мира. По информации, представленной международными экспертами, в итоге названной кибератаки в Российской Федерации была нарушена деятельность национальных компьютерных систем ведущих государственных ведомств (МВД, МЧС, РЖД, Сбербанка, «Мегафона»). Эксперт по компьютерной безопасности Варун Бадхвар отметил: «Мы наблюдаем за тем, как разворачивается сценарий киберапокалипсиса… Только за последние 24 часа заражению подверглись 45 тысяч систем в 74 странах» [23]. Посредством другой крупной кибератаки, реализованной в 2017 г., осуществлено массовое внедрение компьютерного вируса Petya, который незаконно блокировал доступ к информации. В 2018 и в 2019 г. ситуация в данной сфере оставалась нестабильной. В 2020 г. в России было зарегистрировано около 1.5 млрд кибератак [24]. За I полугодие 2021 г. число кибератак на национальную критическую инфраструктуру возросло в 2.5 раза, за 60% атак ответственность возложена на прогосударственных хакеров (APT – Advanced Persistent Threat).

На мировом уровне в 2021 г. количество кибератак имело рост в целом на 150% (в 2020 г. данный показатель по отношению к 2019 г. составил 40%) [25].

В России социально-правовая обусловленность криминализации деяний, вызванных кибератаками, связана со всеобщей цифровизацией, компьютеризацией общества, с ростом нарушений в сфере отношений собственности, с угрозами мировой, национальной и личной безопасности, с ненадлежащим формированием систем информационной безопасности, в частности системы защиты программного обеспечения (СЗПО). Уголовная ответственность за общественно опасные посягательства в сфере компьютерной информации наступает по соответствующим нормам отдельной гл. 28 УК РФ: во-первых, незаконный доступ к информации, содержащейся в компьютере (ст. 272 УК РФ), во-вторых, формирование, применение и распространение компьютерных программ вредоносного характера (ст. 273 УК РФ), в-третьих, нарушение установленных правил в отношении

эксплуатации средств хранения и обработки либо передачи информации компьютера и информационно-телекоммуникационных сетей, распространение порнографических материалов (ст. 274 УК РФ); в-четвертых, неправомерное воздействие на национальную критическую информационную платформу (ст. 274.1 УК РФ).

Так, в рамках уголовно-правовой оценки названных деяний для правильной их квалификации необходимо учитывать следующее:

– при фактах DDoS-кибератак на сайты в сети Интернет юридических лиц, связанных с требованием выплаты определенной суммы денежных средств за снятие блокировки информации, квалификация преступления осуществляется по определенным частям ст. 273 УК РФ;

– при фактах установки контрафактных программ на стационарные либо на мобильные технические устройства — по определенным частям ст. 272, 273 УК РФ;

– при фактах совершения хищений денег из банкоматов с применением различных компьютерных вирусов, контроля над программным обеспечением соответствующего банкомата для отключения связи банкомата с банком и для незаконной выдачи денег – по ст. 159.6, 273, 274 УК РФ [26].

Значительное распространение в России получили киберпреступления, совершенные в форме хищений с применением электронных систем платежа (кража – п. «г» ч. 3 ст. 158, мошенничество – ст. 159.3, п. «в» ч. 3 ст. 159.6 УК РФ). Социально-правовая обусловленность криминализации данных деяний связана с развитием информационно-коммуникационных технологий в области финансовых и банковских услуг, с нарушением охраняемой законом банковской тайны [27], с потребностью активизации уголовно-правовой охраны отношений в области оборота электронных средств, а также с необходимостью обособления данных хищений от смежных преступлений и от административных и гражданско-правовых правонарушений. Так, гр. Т. приговором Северского городского суда Томской области от 19 октября 2020 г. был признан виновным в совершении тайного хищения денежных средств с соответствующего банковского счета (п. «г» ч. 3 ст. 158 УК РФ) из корыстных побуждений посредством использования услуги «мобильный банк» и перевода с чужого банковского счета на личный счет банковской карты денежных средств на общую сумму 51119 руб.; тем самым был причинен значительный материальный ущерб потерпевшему [28].

К категории наиболее общественно опасных киберпреступлений необходимо отнести склонение к совершению самоубийства или содействие совершению названного акта (ст. ст. 110.1, 110.2 УК РФ). Данные вопросы чрезвычайно актуальны. Так, в 2020 г. Россия занимала второе место по числу суицидов (31 случай на 100 000 человек) после Литвы (31.9 человек на 100 000), что обусловлено негативным воздействием на личность в сети Интернет. Российская Федерация в обозначенном направлении обогнала по статистике Гайану (29.2 на 100 000 человек), Корею (26.9), Беларусь (26.2), Суринам (22.8), Казахстан (22.5), Украину (22.4), Лесото (21.2) [29]. Особую озабоченность вызывают суициды несовершеннолетних. По информации, которая предоставлена в конце 2021 г. Межведомственной комиссией, созданной при Совете безопасности РФ, за I полугодие 2021 г. в Российской Федерации было зарегистрировано 3064 случая завершенных актов суицида лиц возраста несовершеннолетия, основная часть которых обусловлена воздействием на личность через сеть Интернет, в т.ч. посредством влияния многочисленных «групп смерти» («разбуди меня в 4:20», «Космический кит», «Море китов», «Океан китов», «Белый кит», «Китовой журнал», «Летающий кит», «f57» и пр.) (+43% по сравнению с 2020 г. (2146)) [30].

Несмотря на сложность розыска субъектов подобных преступлений, суды рассматривают значительное количество уголовных дел. Так, на основании приговора, вынесенного Собинским городским судом Владимирской области, гр. гр. Ш. и Г. признаны виновными по п. «а, в, г, д» ч. 3 ст. 110.1, ч. 2 ст. 110.2 УК РФ за вовлечение лиц возраста несовершеннолетия в игру в сети Интернет, характеризующуюся суицидальной направленностью. По материалам уголовного дела, в августе 2017 г. гр. Ш. в одной из социальных сетей была организована виртуальная «игра смерти», сущность которой – реализация лицами возраста несовершеннолетия определенных заданий, имеющих направленность на личное причинение телесных повреждений и на психическое воздействие на личность. Окончание игры сопровождалось совершением акта самоубийства. В целях реализации преступного умысла гр. Ш. был привлечен ее брат гр. Г., выразивший согласие на предоставление гр. Ш. помощи в поиске в сети Интернет потенциальных «игроков» («китов») в лице несовершеннолетних, пребывающих в сложной жизненной ситуации, и в осуществлении контроля за их поведением. В связи с пресечением преступной деятельности правоохранительными органами акт суицида не был реализован [31].

К категории киберпреступлений, значительных по последствиям, относятся также акты

секстинга (совершение развратных действий в отношении несовершеннолетних, вовлечение в действия сексуального характера; «интернет-педофилия» и пр.). Нередко в судебной практике рассматриваются уголовные дела по преступлениям, которые квалифицированы по ст. ст. 135, 242 УК РФ и обусловлены знакомствами с лицами возраста несовершеннолетия в социальных сетях с целью осуществления переписки эротической направленности и интимного общения по видео-интернет-связи, а также для реализации видеосъемок порнографического характера [32]. Так, приговором Привокзального районного суда г. Тулы, вынесенным 1 октября 2018 г., отмечено, что гр. Б. признан виновным в совершении преступления, квалифицированного по п. «б» ч. 3 ст. 242 УК РФ за факт распространения в сети Интернет материалов порнографического характера в отношении лица возраста несовершеннолетия посредством применения средств массовой информации, в частности информационно-телекоммуникационной сети Интернет [33].

Группу особо общественно опасных киберпреступлений составляет также незаконный сбыт наркотических, психотропных средств и веществ, реализуемый посредством сети Интернет (ч. 2 п. «б» ст. 228-1 УК РФ). О негативном влиянии данного преступления свидетельствуют национальные статистические данные: число лиц, умерших от потребления названных средств и веществ, в 2019 г., составило 4570 человек, что больше на 2.8%, чем в 2018 г. (4445 человек). В 2020 г. данный показатель составляет на 20% больше, чем в 2019 г. В 2021 г. (на ноябрь) в России смертность от употребления увеличилась на 25% [34].

Незаконный оборот наркотических, психотропных средств и веществ посредством использования возможностей сети Интернет осуществляется преимущественно размещением интернет-сообщений в социальных сетях. В качестве преступных инструментов, которые обеспечивают противозаконный оборот названных средств и веществ, значительно увеличивая доступность их получения для целей немедицинского потребления, выступают сегмент сети Интернет, скрытый из общего доступа, «Даркнет» (DarkNet), а также электронные кошельки. Так, приговором Санкт-Петербургского городского суда от 24 апреля 2020 г. гр. гр. К.А., К.Д., Г., С.А. и В. были признаны виновными по ст. ст. 228, 228.1 УК РФ за преступление, совершенное в составе созданной организованной группы (незаконный оборот наркотических средств и психотропных веществ в различных размерах, в т.ч. посредством применения возможностей сети Интернет). Из материалов уголовного дела следует: указанными лицами в преступных целях на основе торговой интернет-площадки был учрежден анонимный интернет-магазин под названием «Квест». Передача наркотических, психотропных средств и веществ от участников организованной преступной группы осуществлялась бесконтактно посредством размещения объектов в тайники. Денежные расчеты осуществлялись путем использования криптовалюты «биткоин» [35].

Особого внимания со стороны субъектов противодействия преступности заслуживают вовлечение несовершеннолетних в преступную деятельность (ст.150 УК РФ) посредством интернет-воздействия, а также публичные призывы к осуществлению экстремистской деятельности (ч. 2 ст. 280 УК РФ). Под подобными призывами понимается активное обращение (агитация) с использованием сети Интернет для оказания воздействия на личность и склонения к экстремистским действиям. Призывы могут быть выражены в выступлениях на митингах, собраниях, иных массовых мероприятиях, в форме экстремистских лозунгов во время демонстраций, шествий и пр. Данный вопрос актуален: в 2020 г. в Российской Федерации было зарегистрировано 2342 экстремистских деяния (+29.7% по сравнению с 2019 г.). В 2021 г. на четверть возросло количество выявленных уголовно наказуемых деяний в сфере противодействия преступным проявлениям экстремизма (с 833 до 1057), однако только треть из них совершена в 2021 г. (355). При этом значительная часть зарегистрированных в России деяний экстремистской направленности была связана именно с публичными призывами к осуществлению такой деятельности (+32.4%, 486), из которых 456 преступлений совершено с использованием сети Интернет [36].

Полагаем, что в зависимости от вида киберпреступления и личности киберпреступников возможно классифицировать на отдельные типы: идеологический тип (распространение сведений экстремистского характера, пр.); корыстный тип (предмет посягательств – как денежные средства, включая виртуальные, использование поддельных документов, так и предметы, характеризующиеся ценностью в киберпространстве (например, предметы игры)); насильственный тип (склонение к суициду, к другому убийству, к причинению вреда посредством как запугивания, так и шантажа, пр.); сексуальный тип (распространение в сети Интернет материалов порнографической направленности, вовлечение в действия развратного сексуального характера и пр.); исследовательский тип (характе-

ризующийся самоутверждением, приобретением особого статуса в сети Интернет посредством реализации кибератак, формирования вредоносных вирусов, и пр.) [37].

В связи со значительными киберугрозами личной, национальной и мировой безопасности наука криминология уделяет особое внимание вопросам противодействия киберпреступности, изучению причин и условий посягательств, личности преступника.

Так, лица, совершающие киберпреступления, дифференцированы на определенные типы, учитывающие уровень вовлеченности в преступную деятельность:

– во-первых, начинающий тип киберпреступника (средний материальный достаток, возможность владеть компьютерными устройствами (одним или более); возраст – от восемнадцати до тридцати лет; преимущественно лица мужского пола с техническим образованием (среднее, среднее специальное или высшее (в ряде случаев – неоконченное)); деятельность – либо профессиональная деятельность, коррелирующая с информационными и компьютерными технологиями (специалисты компьютерных фирм, администраторы баз данных и т.д.), либо отсутствие постоянной работы);

– во-вторых, устойчивый тип киберпреступника (средний и выше среднего материальный достаток, наличие глубоких познаний в сфере информационных технологий, сетей, иных достижений цифрового общества; возраст – средний, от двадцати до двадцати пяти лет; преимущественно мужской пол с тенденцией проявления активности лиц женского пола (5%); образование – преимущественно – высшее техническое или аналогичное неоконченное высшее; наличие возможности владеть инновационными компьютерными системами, устройствами, компьютерными разработками);

– в-третьих, профессиональный тип (высокий уровень материальной обеспеченности; возраст – выше двадцати пяти лет; преимущественно лица мужского пола (доля лиц женского пола – 8%); образование – высшее техническое, наличие профессиональных познаний, навыков, умений в сфере информационных технологий, сетей, иных достижений цифрового общества на высоком уровне, постоянное совершенствование навыков в сфере применения средств для совершения киберпреступлений, в т.ч. разработанных лично) [38, с. 50–52].

Киберпреступление, следовательно, представляет общественно опасное деяние, совершенное в электронной сфере посредством применения информационно-коммуникационных технологий, ресурсов компьютерной информации, т. е. компьютерной системы либо сети, непосредственно – в названной системе либо в сети, либо против названных объектов, посягающее в т. ч. на национальную и мировую безопасность (кибертерроризм и пр.), имущество, имущественные права (кражи, мошенничество в киберпространстве), личную безопасность (кибербуллинг, секстинг, груминг, троллинг и пр.), интеллектуальную собственность (плагиат и киберпиратство) и пр. Характерные признаки киберпреступности: общественная опасность, латентность, оперативность, удаленность, масштабность и высокая анонимность, самодостаточность, виртуальность.

Полагаем, что с целью нивелирования киберугроз и более эффективного противодействия киберпреступности необходимо: совершенствование законодательства и правоприменительной практики, более прогрессивное международное сотрудничество; формирование единой базы данных о киберугрозах; виктимологическая профилактика и правовая, информационная грамотность населения; обеспечение безопасности информационно-коммуникационной сферы (внедрение искусственного интеллекта, создание единой национальной системы противодействия кибератакам, профессиональная подготовка и переподготовка сотрудников правоохранительных органов в сфере информационных технологий, противодействие системе «Даркнет» (DarkNet), преимущественно в которой происходит незаконный оборот криптовалюты, распространение порнографических материалов, сбыт наркотических и психотропных средств, веществ, оружия, взрывчатки).

Список литературы

1. Анисимова А.С. К вопросу о понятии сети «Интернет» в теории права и законодательстве // Юридическая наука. 2015. № 4. С. 5–8.

2. Буз С.И. Киберпреступления: понятие, сущность и общая характеристика // Юристъ-Правоведъ. 2019. № 4 (91). С. 78–82.

3. Лагутин П.Д. Киберпреступность как актуальная угроза обществу // Молодой ученый. 2018. № 42 (228). С. 108–109. URL: https://moluch.ru/archive/228/53137/ (дата обращения: 22.01.2022).

4. Доклад X Конгресса ООН по предупреждению преступности и обращению с правонарушителями // Десятый Конгресс ООН по предупреждению преступности и обращению с правонарушителями. URL: https://www.unodc.org/documents/congress/Previous (дата обращения: 22.01.2022).

5. Organized crime in Europe: the threat of cybercrime. Council of Europe Publishing, 2005. 368 p.

6. Мирончик А.С., Суслопаров А.В. Хищения в электронной среде как разновидность информационных преступлений: проблемы разграничения и квалификации // Юридические исследования. 2019. № 9.

С. 17–30. URL: https://elibrary.ru/item.asp?id=41384717 (дата обращения: 22.01.2022).

7. Бойко О.А., Унукович А.С. Детерминанты латентных преступлений, совершаемых с использованием информационно-телекоммуникационных технологий // Юридический вестник Самарского университета. 2020. № 6 (3). С. 53–59.

8. Состояние преступности в России за январь–декабрь 2021 года / ЦСИ ГИАЦ МВД России.

9. Генеральная прокуратура. Состояние преступности в России. 2019, 2020, 2021 (первое полугодие). URL: https://genproc.gov.ru (дата обращения: 22.01.2022).

10. Овчинский А.С., Шмонин А.В., Торопов Б.А., Васильев Ф.П. Криминальная среда цифрового мира как угроза кибербезопасности // Вопросы безопасности. 2019. № 5. С. 9–15.

11. Президент РФ призвал органы внутренних дел к эффективной защите общества в цифровом пространстве. URL: https://www.garant.ru/news/1449069/ (дата обращения: 22.01.2022).

12. Федеральный закон от 24 июня 1999 г. № 120-ФЗ «Об основах системы профилактики безнадзорности и правонарушений несовершеннолетних» // Собрание законодательства Российской Федерации. 1999. № 26. Ст. 3177.

13. Федеральный закон от 29 декабря 2010 г. № 436-ФЗ «О защите детей от информации, причиняющей вред их здоровью и развитию» // Собрание законодательства Российской Федерации. 2011. № 1. Ст. 48.

14. Указ Президента Российской Федерации от 5 декабря 2016 г. № 646 «Об утверждении Доктрины информационной безопасности Российской Федерации» // Собрание законодательства Российской Федерации. 2016. № 50. Ст. 7074.

15. Указ Президента Российской Федерации от 9 мая 2017 г. № 203 «О Стратегии развития информационного общества в Российской Федерации на 2017 – 2030 годы» [Электронный ресурс]. URL: http://www.pravo.gov.ru. (дата обращения: 10.01.2021).

16. Указ Президента Российской Федерации от 21 июля 2020 г. № 474 «О национальных целях развития Российской Федерации на период до 2030 года» // Российская газета. 2021. 22 июля.

17. Егоров И. Россия внесла в ООН первый проект Конвенции по борьбе с киберпреступностью // Российская газета. 2021. № 168 (8519) [Электронный ресурс] // Официальный сайт Российской газеты. URL: https://rg.ru/2021/07/27/rossiia-vnesla-v-oon-pervyj-proekt-konvencii-po-borbe-s-kiberprestupnostiu.html (дата обращения: 22.01.2022).

18. Конвенция о преступности в сфере компьютерной информации (ETS № 185) (г. Будапешт, 23.11.2001). URL: http://www.consultant.ru/online/ (дата обращения: 22.01.2022).

19. Конвенция Организации Объединенных Наций о противодействии использованию информационно-коммуникационных технологий в преступных целях (проект от 29.06.2021). URL: https://www.kommersant.ru/docs/2021/RF_28_July_2021_-_R.pdf (дата обращения: 22.01.2022).

20. Резолюция Генеральной Ассамблеи ООН от 27 декабря 2019 г. № 74/247 «Противодействие использованию информационно-коммуникационных технологий в преступных целях». URL: https://www.un.org/ru/ga/ (дата обращения: 22.01.2022).

21. Мозжерина В.В. Проблемы ответственности за мошенничество с использованием электронных средств платежа // Сборник материалов VI Международного научно-спортивного фестиваля курсантов и студентов (г. Пермь, 13–18 мая 2019 г.). Пермь: ПИ ФСИН, 2019. С. 120–122.

22. Игнатова О., Куликов В. Кто кого обманывает // Российская газета. 2021. 14 июля. URL: www.Rg-ru.turbopages.org (дата обращения: 22.01.2022).

23. Вирус атаковал компьютерные сети по всему миру. URL: https://www.1tv.ru/news/2017/0513/325215virus_atakoval_kompyuternye_seti_po_vsemu_miru (дата обращения: 22.01.2022).

24. В МИД России зафиксировали в 2020 году более 1 млрд кибератак на цифровые объекты. URL: https://www.advgazeta.ru/novosti/kiberprestupleniy-stanovitsya-vse-bolshe-odnako-ikh-raskryvaemost-umenshaetsya/ (дата обращения: 20.02.2021).

25. 60% кибератак на российские объекты провели работающие на иностранные правительства хакеры. URL: https://www.kommersant.ru/doc/4898519 (дата обращения: 20.02.2021).

26. Евдокимов К.Н., Таскаев Н.Н. Проблемные вопросы квалификации преступлений, предусмотренных статьей 273 УК РФ, на стадии возбуждения уголовного дела // Всероссийский криминологический журнал. 2018. Т. 12. № 4. С. 590–600. URL: https://cyberleninka.ru/article/n/problemnye-voprosy-kvalifikatsii (дата обращения: 20.02.2021).

27. Федеральный закон от 2 декабря 1990 года № 395-1 «О банках и банковской деятельности» // Собрание законодательства Российской Федерации. 1996. № 6. Ст. 492.

28. Определение Восьмого кассационного суда общей юрисдикции от 22 июля 2021 г. № 77-3009/2021. URL: http://www.consultant.ru/cons/cgi/online.cgi?req=doc&base (дата обращения: 22.01.2022).

29. Статистика суицида 2021 г. по странам. URL: https://gidnenuzen.ru/statistika-suitsida-2021-po-stranami/ (дата обращения: 22.01.2022).

30. Совбез РФ: В 2021 году отмечен рост половых преступлений против детей // Российская газета. 2021. 29 ноября.

31. Приговор Собинского городского суда Владимирской области от 10 сентября 2018 г. URL: http://oblsud.wld.sudrf.ru/modules.php?name=press_dep&op=1&did=1528 (дата обращения: 22.01.2022).

32. Степанова О.Ю. Проблемы привлечения к уголовной ответственности за педофилию в социальных сетях // Санкт-Петербургский вестник МВД России. 2015. № 2 (66). С. 78–80. URL: https://cyberleninka.ru/article/n/problema-privlecheniya-k-ugolovnoy (дата обращения: 22.01.2022).

33. Определение Судебной коллегии по уголовным делам Верховного Суда Российской Федерации от 24 декабря 2019 г. № 38-УД19-6. URL: http://www.consultant.ru/cons/cgi/online.cgi?req=doc&base (дата обращения: 22.01.2022).

34. Смертность в России за последний год стала рекордной со времен войны. URL: https://www.vedomosti.ru/society/articles/2021/11/29/898151-umershih-antirekord (дата обращения: 22.01.2022).

35. Апелляционное определение Второго апелляционного суда общей юрисдикции от 11 декабря 2020 г. по делу № 55-592/2020. URL: http://www.consultant.ru/cons/cgi/online.cgi?req=doc&base=SOAS&n=

13168&dst=100177#COMOjnS7Q67YeA3S (дата обращения: 22.01.2022).

36. Генеральная прокуратура РФ, состояние преступности (январь–октябрь 2021 г.). URL: http://crimestat.ru/analytics (дата обращения: 22.01.2022).

37. Косенков А.Н., Черный Г.А. Общая характеристика психологии киберпреступника // Всероссийский криминологический журнал. 2012. 3 (21). С. 87–94. URL: https://cyberleninka.ru/article/n/obschaya-harakteristika-psihologii (дата обращения: 22.01.2022).

38. Гаврило Ю.В., Аносов А.В., Баранов В.В. Деятельность ОВД по борьбе с преступлениями, совершёнными с использованием информационных, коммуникационных и высоких технологий: Учебное пособие. М.: Академия управления МВД России, 2019. Ч. 1. 208 с.

CYBERCRIME: CONCEPT, SIGNS, MAIN DIRECTIONS OF COUNTERACTION

V.B. Klishkov, E.V. Stebeneva, M.A. Yakovleva

The purpose of the article is to study the definition, characteristic features and main directions of countering cybercrime. The article analyzes the concept of the category «cybercrime», the level of public danger of cybercrimes, summarizes the positions regarding the characteristic features of this act, presents the classification of cybercrimes. Results: the article reflects the features of the most socially dangerous cybercrimes, presents their statistical data (in dynamics), the author's vision regarding the definition and signs of this phenomenon, the main directions of countering cybercrime in the Russian Federation.

Keywords: security, cybercrime, cybercrime, cyber threats, identity of a cybercriminal, countering crime.

References

1. Anisimova A.S. On the question of the concept of the Internet in the theory of law and legislation // Legal Science. 2015. № 4. P. 5–8.

2. Buz S.I. Cybercrimes: concept, essence and general characteristics // Jurist-Pravoved. 2019. № 4 (91). P. 78–82.

3. Lagutin P.D. Cybercrime as an actual threat to society // Young Scientist. 2018. № 42 (228). P. 108–109. URL: https://moluch.ru/archive/228/53137/ (Date of access: 22.01.2022).

4. Report of the X UN Congress on the Prevention of Crime and the Treatment of Offenders // The Tenth United Nations Congress on the Prevention of Crime and the Treatment of Offenders. URL: https://www.unodc.org/documents/congress/Previous (Date of access: 22.01.2022).

5. Organized crime in Europe: the threat of cybercrime. Council of Europe Publishing, 2005. 368 p.

6. Mironchik A.S., Susloparov A.V. Embezzlement in the electronic environment as a kind of information crimes: problems of differentiation and qualification // Legal research. 2019. № 9. P. 17–30. URL: https://elibrary.ru/item.asp?id=41384717 (Date of access: 22.01.2022).

7. Boyko O.A., Unukovich A.S. Determinants of latent crimes committed with the use of information and telecommunication technologies // Legal Bulletin of the Samara University. 2020. № 6 (3). P. 53–59.

8. The state of crime in Russia for January–December 2021 / CSI GIAC of the Ministry of Internal Affairs of Russia.

9. The Prosecutor General's Office. The state of crime in Russia. 2019, 2020, 2021 (first half of the year). URL: https://genproc.gov.ru (Date of access: 22.01.2022).

10. Ovchinsky A.S., Shmonin A.V., Toropov B.A., Vasiliev F.P. Criminal environment of the digital world as a threat to cybersecurity // Security issues. 2019. № 5. P. 9–15.

11. The President of the Russian Federation called on the internal affairs bodies to effectively protect society in the digital space. URL: https://www.garant.ru/news/1449069/ (Date of access: 22.01.2022).

12. Federal Law № 120-FL of June 24, 1999 «On the fundamentals of the system of prevention of lack of supervision and offenses of imperfect years» // Collection of Legislation of the Russian Federation. 1999. № 26. Art. 3177.

13. Federal Law of December 29, 2010 № 436-FL «On the protection of children from information harmful to their health and development» // Collection of Legislation of the Russian Federation. 2011. № 1. Art. 48.

14. Decree of the President of the Russian Federation № 646 of December 5, 2016 «On the approval of the Information Security Doctrine of the Russian Federation» // Collection of Legislation of the Russian Federation. 2016. № 50. Art. 7074.

15. Decree of the President of the Russian Federation dated May 9, 2017 № 203 «On the Strategy for the development of the Information Society in the Russian Federation for 2017–2030» [Electronic resource]. URL: http://www.pravo.gov.ru (Date of access: 10.01.2021).

16. Decree of the President of the Russian Federation № 474 of July 21, 2020 «On the national development goals of the Russian Federation for the period up to 2030» // Rossiyskaya Gazeta. 2021. July 22.

17. Egorov I. Russia has submitted to the UN the first draft of the Convention on Combating Cybercrime // Rossiyskaya Gazeta. 2021. № 168 (8519) [Electronic resource] // Official website of the Russian newspaper. URL: https://rg.ru/2021/07/27/rossiia-vnesla-v-oon-pervyj-proekt-konvencii-po-borbe-s-kiberprestupnostiu.html (Date of access: 22.01.2022).

18. Convention on Computer Information Crime (ETS № 185) (Budapest, 23.11.2001). URL: http://www.consultant.ru/online/ (Date of access: 22.01.2022).

19. United Nations Convention on Countering the Use of Information and Communication Technologies for Criminal Purposes (draft dated 29.06.2021). URL: https://www.kommersant.ru/docs/2021/RF_28_July_2021_-_R.pdf (Date of access: 22.01.2022).

20. UN General Assembly Resolution № 74/247 of December 27, 2019 «Countering the use of information and communication technologies for criminal purposes».

URL: https://www.un.org/ru/ga/ (Date of access: 22.01.2022).

21. Mozzherina V.V. Problems of liability for fraud using electronic means of payment // Collection of materials of the VI International Scientific and Sports Festival of cadets and students (Perm, May 13–18, 2019). Perm: PI FSIN, 2019. P. 120–122.

22. Ignatova O., Kulikov V. Who is deceiving whom // Rossiyskaya Gazeta. 2021. July 14. URL: www.Rg-ru.turbopages.org (Date of access: 22.01.2022).

23. The virus attacked computer networks around the world. URL: https://www.1tv.ru/news/2017/0513/325215virus_atakoval_kompyuternye_seti_po_vsemu_miru (Date of access: 22.01.2022).

24. The Russian Foreign Ministry recorded more than 1 billion cyber attacks on digital objects in 2020. URL: https://www.advgazeta.ru/novosti/kiberprestupleniy-stanovitsya-vse-bolshe-odnako-ikh-raskryvaemost-umenshaetsy/ (Date of access: 20.02.2021).

25. 60% of cyberattacks on Russian facilities were carried out by hackers working for foreign governments. URL: https://www.kommersant.ru/doc/4898519 (Date of access: 20.02.2021).

26. Evdokimov K.N., Taskaev N.N. Problematic issues of qualification of crimes stipulated by Article 273 of the Criminal Code of the Russian Federation at the stage of initiation of a criminal case // All-Russian Criminological Journal. 2018. Vol. 12. № 4. P. 590–600. URL: https://cyberleninka.ru/article/n/problemnye-voprosy-kvalifikatsii (Date of access: 20.02.2021).

27. Federal Law № 395-1 of December 2, 1990 «On Banks and banking activities» // Collection of Legislation of the Russian Federation. 1996. № 6. Art. 492.

28. Ruling of the Eighth Cassation Court of General Jurisdiction dated July 22, 2021 № 77-3009/2021. URL: http://www.consultant.ru/cons/cgi/online.cgi?req=doc&base (Date of access: 22.01.2022).

29. Suicide statistics 2021 by country. URL: https://gidnenuzen.ru/statistika-suitsida-2021-po-stranami/ (Date of access: 22.01.2022).

30. The Security Council of the Russian Federation: In 2021, there was an increase in the number of crimes against children // Rossiyskaya Gazeta. 2021. November 29.

31. The verdict of the Sobinsky City Court of the Vladimir region of September 10, 2018. URL: http://oblsud.wld.sudrf.ru/modules.php?name=press_dep&op=1&did=1528 (Date of access: 22.01.2022).

32. Stepanova O.Yu. Problems of bringing to criminal responsibility for pedophilia in social networks // St. Petersburg Bulletin of the Ministry of Internal Affairs of Russia. 2015. № 2 (66). P. 78–80. URL: https://cyberleninka.ru/article/n/problema-privlecheniya-k-ugolovnoy (Date of access: 22.01.2022).

33. Ruling of the Judicial Board on Corner Cases of the Supreme Court of the Russian Federation dated December 24, 2019 № 38-UD19-6. URL: http://www.consultant.ru/cons/cgi/online.cgi?req=doc&base (Date of access: 22.01.2022).

34. Mortality in Russia over the past year has become a record since the war. URL: https://www.vedomosti.ru/society/articles/2021/11/29/898151-umershih-antirekord (Date of access: 22.01.2022).

35. Appeal ruling of the Second Court of Appeal of General Jurisdiction dated December 11, 2020 in case № 55-592/2020. URL: http://www.consultant.ru/cons/cgi/online.cgi?req=doc&base=SOAS&n=13168&dst=100177#COMOjnS7Q67YeA3S (Date of access: 22.01.2022).

36. Prosecutor General's Office of the Russian Federation, state of emergency (January–October 2021). URL: http:// crimestat.ru/analytics (Date of access: 22.01.2022).

37. Kosenkov A.N., Cherny G.A. General characteristics of cybercriminal psychology // All-Russian Criminological Journal. 2012. 3 (21). P. 87–94. URL: https://cyberleninka.ru/article/n/obschaya-harakteristika-psihologii (Date of access: 22.01.2022).

38. Gavrilo Yu.V., Anosov A.V., Baranov V.V. Activities of the Department of Internal Affairs to combat crimes committed using information, communication and high technologies: Textbook. M.: Academy of Management The Ministry of Internal Affairs of Russia, 2019. Part 1. 208 p.